使用AMP on FireSIGHT管理中心排除連線和註冊問題

目錄

簡介

部署中的FireSIGHT管理中心可以連線到思科雲。配置FireSIGHT管理中心以連線到雲後，您可以接收掃描、惡意軟體檢測和隔離的記錄。記錄作為惡意軟體事件儲存在FireSIGHT管理中心資料庫中。預設情況下，雲會為組織中的所有組傳送惡意軟體事件，但您可以在配置連線時按組進行限制。本檔案將討論FireSIGHT管理中心高級惡意軟體防護(AMP)功能的各種問題和疑難排解步驟。

防火牆中的埠或伺服器被阻止

如果FireSIGHT管理中心無法連線到FireAMP雲控制檯，或者沒有收到惡意軟體事件，則必須檢查所需的埠是否被防火牆阻塞。FireSIGHT管理中心使用埠443從FireAMP控制檯接收基於終端的惡意軟體事件。FirePOWER裝置32137思科雲中執行惡意軟體查詢時需要埠資訊。

要瞭解有關所需埠號和伺服器地址的詳細資訊，請閱讀以下文檔：

- FireSIGHT系統運行所需的通訊埠
- AMP操作所需的伺服器

正在使用的MAC地址

症狀

當您嘗試將FireSIGHT管理中心註冊到私有雲並執行初始連線時，可能會收到一條消息，指示MAC地址已在使用中。

原因

如果由於硬體故障而更換FireSIGHT管理中心，且未從雲中正確註銷更換單元，則可能會遇到此問題。

解決方案

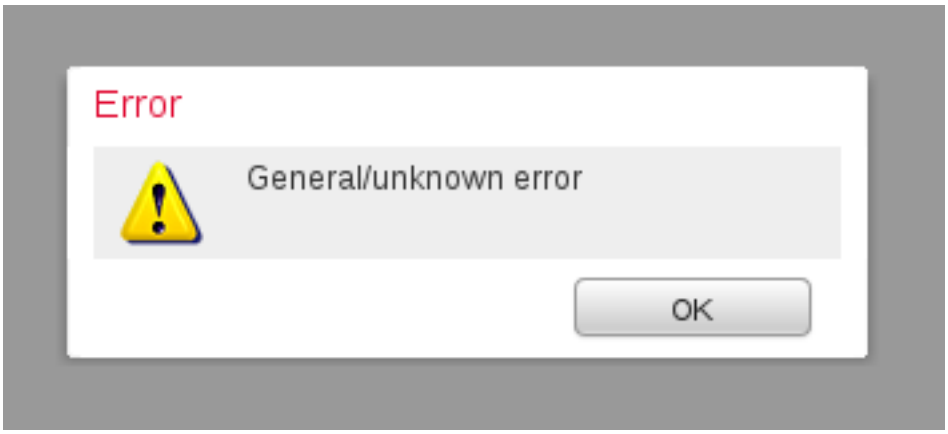
在更換裝置之前，您必須從FireAMP雲註銷FireSIGHT管理中心。您還應從FireAMP雲中刪除FireSIGHT管理中心。這可防止將MAC地址視為正在使用。

> **提示：**閱讀本文檔，瞭解有關如何從FireAMP雲註銷裝置和從FireSIGHT管理中心刪除雲的詳細流程。

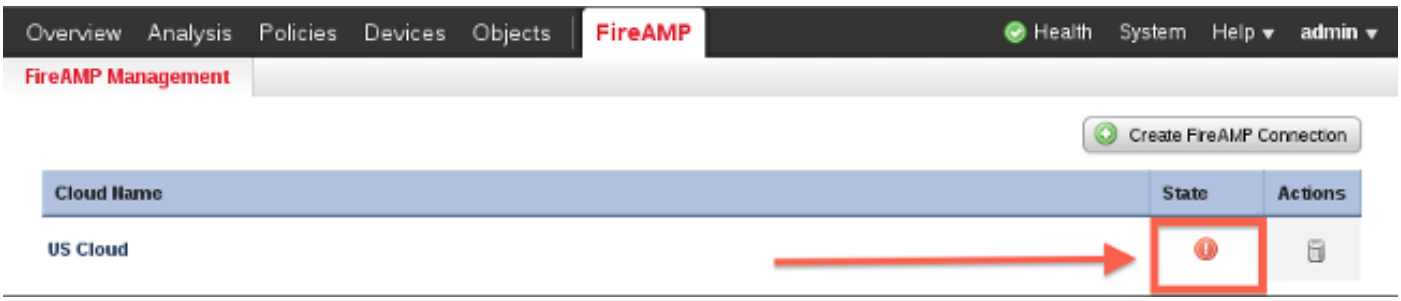
顯示常規/未知錯誤

症狀

將重新映像或更換的FireSIGHT管理中心連線到FireAMP控制檯時，將顯示錯誤消息。它會顯示General/unknown錯誤。



當出現General/unknown error消息時，FireSIGHT管理中心上的FireAMP連線的狀態變為嚴重。Web介面顯示一個紅色圖示。



原因

當FireSIGHT管理中心的MAC地址（已重新映像或替換）仍註冊到FireAMP控制檯時，會發生此問題。

解決方案

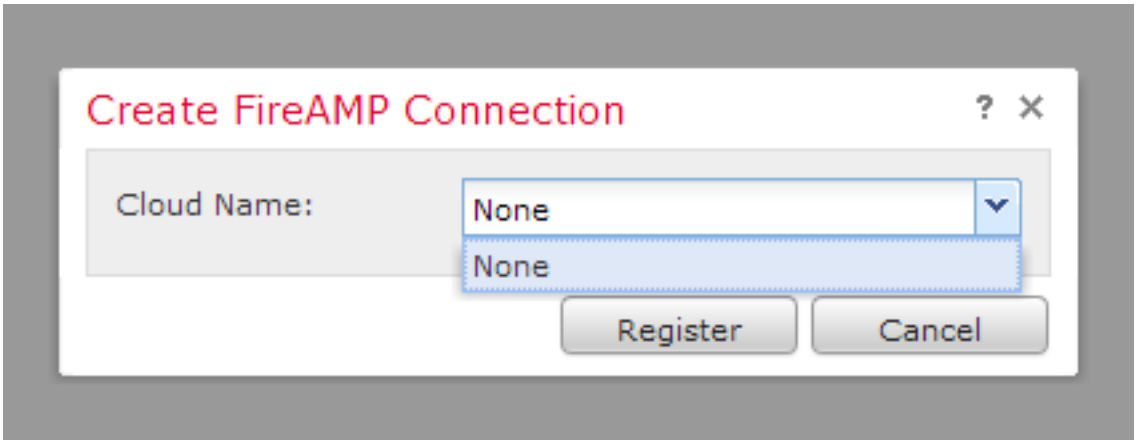
在重新映像或更換裝置之前，您必須從FireAMP雲註銷FireSIGHT管理中心。您還應從FireAMP雲中刪除FireSIGHT管理中心。這可防止將MAC地址視為正在使用。

> **提示：**閱讀本文檔，瞭解有關如何從FireAMP雲註銷裝置和從FireSIGHT管理中心刪除雲的詳細流程。

無法選擇雲

症狀

建立從FireSIGHT管理中心到FireAMP雲控制檯的連線時，找不到適用於美國雲或歐盟雲的下拉選項。



原因

當FireSIGHT管理中心無法解析主機名api.amp.sourcefire.com時，會發生此問題。

若要驗證問題，請在FireSIGHT管理中心的CLI上執行nslookup。檢查FireSIGHT管理中心上是否正確配置了DNS設定：

```
admin@Sourcefire3D:~$ sudo nslookup api.amp.sourcefire.com
```

當DNS無法解析FireSIGHT管理中心上的主機名時，將顯示以下輸出：

```
admin@Sourcefire3D:~$ sudo nslookup api.amp.sourcefire.com

Server:         192.168.45.2
Address:        192.168.45.2#53

** server can't find api.amp.sourcefire.com
```

如果在FireSIGHT管理中心上正確解析了DNS，則輸出如下：

```
admin@Sourcefire3D:~$ sudo nslookup api.amp.sourcefire.com
```

```
Server:         192.168.45.1
Address:        192.168.45.1#53

Non-authoritative answer:
api.amp.sourcefire.com
Name:   xxxx.xxxx.xxxx
Address: xx.xx.xx.xx
```

解決方案

- 如果FireSIGHT管理中心無法解析主機名，則需要驗證管理中心上的DNS設定是否正確。
- 如果FireSIGHT管理中心能夠解析主機名，但無法通過防火牆訪問api.amp.sourcefire.com，請檢查防火牆規則和設定。

在連線建立過程中，如果FireSIGHT管理中心無法解析主機名，以下錯誤消息將記錄在httpsd_error_log中：

Error attempting curl for FireAMP: System

例如，以下日誌輸出顯示Defense Center無法完成api.amp.sourcefire.com的curl命令：

```
admin@Sourcefire3D:~$ tail -f /var/log/httpd/httpsd_error_log

[Thu Jul 18 12:38:13.433765 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
getCloudData start... at /usr/local/sf/lib/perl/5.10.1/SF/Permission.pm line 1778., referer:
https://192.168.45.45/ddd/
[Thu Jul 18 12:38:14.338174 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
/usr/local/bin/curl -s --connect-timeout 10 -m 20 -L --max-redirs 5 --max-filesize 104857600 --
sslv3 --capath /etc/sf/keys/fireamp/thawte_roots/ -H Accept:
application/vnd.sourcefire.fireamp.dc+json; version=1 https://api.amp.sourcefire.com/clouds at
/usr/local/sf/lib/perl/5.10.1/SF/System.pm line 7491., referer: https://192.168.45.45/ddd/
[Thu Jul 18 12:38:24.352374 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
Error attempting curl for FireAMP: System (/usr/local/bin/curl -s --connect-timeout 10 -m 20 -L
--max-redirs 5 --max-filesize 104857600 --sslv3 --capath /etc/sf/keys/fireamp/thawte_roots/ -H
Accept: application/vnd.sourcefire.fireamp.dc+json; version=1
https://api.amp.sourcefire.com/clouds) Failed at /usr/local/sf/lib/perl/5.10.1/SF/System.pm line
7499., referer: https://192.168.45.45/ddd/
[Thu Jul 18 12:38:24.352432 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
No cloud data returned at /usr/local/sf/lib/perl/5.10.1/SF/FireAMP.pm line 145., referer:
https://192.168.45.45/ddd/
[Thu Jul 18 12:38:24.352478 2013] [cgi:error] [pid 10920] [client 192.168.45.50:59220] AH01215:
getCloudData completed... at /usr/local/sf/lib/perl/5.10.1/SF/Permission.pm line 1780., referer:
https://192.168.45.45/ddd/
```

在連線建立過程中，如果以下消息記錄在httpsd_error_log中而沒有錯誤，則表明FireSIGHT管理中心能夠解析主機名：

```
getCloudData completed
```

例如，以下輸出顯示，管理中心完成對api.amp.sourcefire.com的curl命令：

```
admin@Sourcefire3D:~$ tail -f /var/log/httpd/httpsd_error_log

[Thu Jul 18 12:42:54.949461 2013] [cgi:error] [pid 12007] [client 192.168.45.50:59253] AH01215:
getCloudData start... at /usr/local/sf/lib/perl/5.10.1/SF/Permission.pm line 1778., referer:
```

https://192.168.45.45/ddd/
[Thu Jul 18 12:42:55.856432 2013] [cgi:error] [pid 12007] [client 192.168.45.50:59253] AH01215: /usr/local/bin/curl -s --connect-timeout 10 -m 20 -L --max-redirs 5 --max-filesize 104857600 --sslv3 --capath /etc/sf/keys/fireamp/thawte_roots/ -H Accept: application/vnd.sourcefire.fireamp.dc+json; version=1 https://api.amp.sourcefire.com/clouds at /usr/local/sf/lib/perl/5.10.1/SF/System.pm line 7491., referer: https://192.168.45.45/ddd/
[Thu Jul 18 12:42:55.931106 2013] [cgi:error] [pid 12007] [client 192.168.45.50:59253] AH01215: **getCloudData completed**... at /usr/local/sf/lib/perl/5.10.1/SF/Permission.pm line 1780., referer: https://192.168.45.45/ddd/